Australian Journal of Basic and Applied Sciences, 9(10) Special 2015, Pages: 107-114

ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com

Layering Approach for Developing A Secured Infra-Structure Model for Cloud Environment

Roopa and Emilin Shyni

KCG College of Technology, Chennai, India, 600097

ARTICLE INFO

Article history:
Received 28 January 2015
Accepted 25 February 2015
Available online 6 March 2015

Keywords:
Cloud, Data, Data Security- Random Number Generation, Detection Algorithm, Security- Access Control.

ABSTRACT

There are two fundamental aspects that Cloud has transformed in this information age- Storage and Security. Cloud reach is also limited by these two factors. The term Information Age is that data(information) is available abundantly. There is tremendous increase for the Cloud users to store and access the data. Hence it becomes a necessity that cloud providers to build a trust enabled relationship to the tenants. This is the biggest challenge that the cloud evangelists and becomes a priority to be addressed. This aspect has revolutionized the operations of Information Technology. Exchange of information becoming a necessity the focus turns on security. The data, from the point of creation to archiving, the travel is on different layers across the network. Storage and retrieval also is taking place inside the cloud network. Hence this paper provides the architecture for layered approach to secure the cloud network. Data aberration detection algorithm is highlighted ensuring data integrity in cloud. Private, public and hybrid cloud networks can implement this effective model in the network.

To Cite This Article: Roopa and Emilin Shyni, Layering Approach for Developing A Secured Infra-Structure Model for Cloud Environment. ***Aust. J. Basic & Appl. Sci.,*** *9(10): 107-114, 2015*

INTRODUCTION

Cloud computing is emerging in almost all kinds of business organizations and is expected to grow in this random manner. The concept of virtualization is the key aspect of using any cloud computing service. Cloud computing is a term that brings all the services that the cloud can offer and the computing is on the internet(cloud) layer. The major advantage that computing offers is that the selection of services and the usage can be defined anytime and is a flexible architecture to handle. The other aspect of cloud is the Cloud deployment model classification. The Public Cloud is where the major cloud providers have their services on public network (Internet) and a simple login and pay is made by the users to have access to these services. But the storage and the access in the public cloud is of major security concern as it's the most vulnerable model in cloud.

The private cloud is a well- defined cloud model implemented in private sectors with network access scenario and the utilization of services are also monitored in this model.

For better utilization of services and to have a more flexible model the Hybrid clouds are deployed where in the user access and the service provider access are all on the same network. This model can clearly make a border-line and the computing is also monitored. This distinguishing factor of hybrid cloud is a major advantage of being cost- effective, the overall utilization and service provided is beneficial and is available to users whenever needed and the efficiency and performance of this hybrid model is very high when compared to other cloud models.

The major services provided by cloud are SaaS(Software as a Service) where the need for installing a software or the need to use more needed software and even the cost of purchasing the software along with the licensing issues are all done in cloud virtual scenario where the software is provided as a Service.

PaaS(Platform as a Service) where the virtual cloud platform is created and are chosen without a physical hardware on the user but can compute on a virtual hardware.

IaaS(Infrastructure as a Servie) where in all the infrastructures needed like additional storage space, efficient computing processors are all available either as a pre-defined model or can be user-defined.

One major area of concern is that the overall working of the cloud can be clearly known and be used only if it is properly computed, since the concept of cloud computing is all happening in the Virtual scenario (Grobauer, 2011). Hence this set-up makes it complex not in terms of usage but in terms of implementing and addressing the security concerns. The service provider task is not only to

Corresponding Author: KCG College of technology, chennai, India, 600097
E-mail: rooparam81@gmail.com

provide services to the users (Vijay Varadharajan, 2014) but also to have a well defined secured architecture of their model for the users. The overall working of any cloud service model is based on the availability of internet. This internet can have multiple locations for logging in and accessing the cloud. Hence making cloud vulnerable to the security threats. This concept is being implemented and is flexible where-in based on the growth, security measures are altered and then implemented. This process is not a standardized model as it can be implemented based on the various security levels and threats that are being faced in the public and private models.

The attacks are the major security issue in recent times. The attack can be the users of the tenants – the end consumers. If the tenant is a Business Entity in a particular domain (say Healthcare) a malicious tenant could gain unauthorized access to the tenant server where all the Health Records and Patient data is stored by the Healthcare company. This is vulnerability. So the security model should ensure that the users are properly authenticated and authorized when logging-in, storing and retrieving data. Alternatively the attack could even be from the tenant administrator who can use the administrative privileges for malicious reasons and could actually hack the secured hosted resources, databases or even get access to financial resources of the Business. Hence the secured key based authentication and login becomes extremely necessary for a cloud environment, which this paper focuses on.

Security Concerns – Review:

Cloud Security Models:

The security architecture that provides a flexible security as a service model that a cloud provider can offer to its tenants and customers of its tenants. The security services that a cloud provider can offer as part of its infrastructure to its customers (tenants) to counteract attacks. Two types of attack: TSAD, SPAD [7]are analyzed based on the logs of all the running programs in the system provided by them. Each program running is given a unique Process ID and based on this scheme the logs are verified. Pro_Val and Re_virt techniques are implemented based on the spec of SPAD module implemented in Sophos tool. The insider attacks from both tenant and service provider end is analyzed, TCP SYN flooding attacks, spoofing attacks and the implementation of the architecture is made on XEN Hypervisor. The model provides flexibility to tenants to have additional security functionalities that suit their security requirements. But the focus on data and related security measures on data storage is not of much significance.

A comprehensive review of the existing security and privacy issues in cloud environments is proposed (Zhifeng Xiao and Yang Xiao, 2013). The cloud environment has been considered as a new computing platform to which the classic methodology of security research can be applied as well. Therefore, focus is to employ an attribute-driven methodology and the ecosystem of cloud security and privacy in view of five security/privacy attributes (i.e., confidentiality, integrity, availability, accountability, and privacy- preservability), that are the most representative ones in current research advances. Data and business application outsourced to a third party causes the security and privacy issues to become a critical concern. These attributes, the relationships, the vulnerabilities that may be exploited by attackers, the threat models, as well as existing defense strategies in a cloud scenario.

The advancements in the Security and Privacy considerations of the cloud is also a topic of discussion (Kwang Mong, 2012). Identification of new threats and vulnerabilities, protecting the virtual infrastructure and outsourced computations and services. The focus is also on the user data and security of big data access and control. The flexibility of cloud model and the various cryptography, virtualization, data management to be improvised based on the requirements to be provided.

Cloud storage arises a lot of concerns towards security and data integrity (Cong Wang, 2012). Cryptographic primitives are implemented for the purpose of data integrity. The existing system has an effective and flexible distributed storage and hence the verification is done with explicitly dynamic data support. The stored data are in encrypted file formats and these files support modifications like: update, delete and append. To achieve the assurances of cloud data integrity and availability and enforce the quality of dependable cloud storage service for users, we propose an effective and flexible distributed scheme with explicit dynamic data support, including block update, delete, and append. The calculation of computations is based on the changes in original files and modified files to give the appended block.

B. Cloud Security & Architecture Models:

User Trusted Entity (UTE) the proposed approach is supposed to make cloud computing infrastructures reliable in order to enable infrastructure service developers to provide a closed execution environment. One advantage of the proposed UTE is that managers of Infrastructure as a Service (IaaS) systems have no privilege within UTE. The most important advantage of UTE is that system administrators managing IaaS do not have any privilege so that none of them can intervene in the functionality of TC. It is assumed in this paper that UTE is maintained by a third agent with no incentive to collude and also highly trusted with IaaS server. This ensures the confidential running of guest VMs and also let the users verify IaaS server and before VM start-up check if the presented cloud server is safe or not.

Access control model is the role-based access control (RBAC), which provides flexible controls and management by having two mappings, users to roles and roles to privileges on data objects (Lan Zhou, 2013). A role- based encryption (RBE) scheme that integrates the cryptographic techniques with RBAC. The Component Flow: Public Cloud: Private Cloud: User: Role Manager: Administrator: Owner: Secure Communications with inclusions of Encryption and Decryption for data storage.

A novel architecture that integrates cloud database services with data confidentiality and the possibility of executing concurrent operations on encrypted data (Luca Ferretti, 2014). The system proposes a Secure DBaaS as the first solution that allows cloud tenants to take full advantage of DBaaS qualities, such as availability, reliability, and elastic scalability, without exposing unencrypted data to the cloud provider.The cloud computing terminology includes five major characteristics: On-demand self-service, Broad network access, Resource pooling or multi-tenancy, Rapid elasticity, Measured service(pay- as – you- go) and Transitivity. The main assessment strategies are security, privacy, audit and SLA. The pre and post assessment is based on the service utilized by the tenants and service provided to the tenants.

The proposed security model:

"Cloud computing" has truly emerged as the next generation computing, where systems are moved from an "on premise" to "on demand" entities. This has made the companies to re-think and re-engineer the way the businesses are operated and hence leading to transformation. Amazon Web Services and Salesforce are just a couple of the top 2 picks in defining the success of Cloud. But the greatest concern for the "Cloud Computing" to get high acceptance is the questions on the Security of the data that is stored in the Cloud. To address that precise problem this paper proposes four levels of Security in Cloud Environment.

They are:

1. Network Level Security
2. Server Level Security
3. Login Level Security
4. Data Level Security

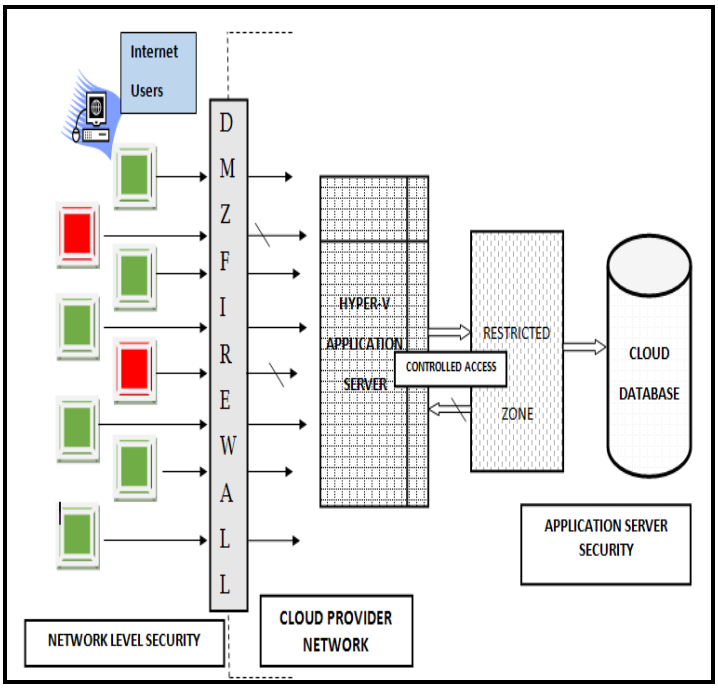

Fig. 1: Network Level Security Architecture.

Firstly, there is a need to analyze why the four layers of Security is required. The Network Level Security is the layer that is the primary level of security that protects the entire system from the external attacks and threats. This level lies at the periphery of the entire network. The next level of security is the Server Level Security where in the paper proposes the recommended server level security in a network so that the actual assets of the system like the servers, databases, applications are secured. Following the Server Level Security, we have the Login Level security, which actually puts a check on who gets into the system (figure 1). The additional feature on the Login level security will be discussed later in the paper. The final and the most critical level of the Security is the Data Level security. In this level, three sub-levels of Security will be discussed to give more security for the Data which is the core aspect of any user. Thus with all these four levels, a high level of Security can be

achieved with the Cloud system, thus minimizing attacks and threats to a great extent and maximizing the Trust of the end users (consumers) on the cloud architecture..

Network Level Security:

To define Network Level Security in simple terms – the policies incorporated and adopted by the IT-Network administrator to prevent attacks, threats and inappropriate usage of network resources from the outside world or external entities. In the present IT landscape and more so with a Cloud System, network security becomes extremely important as this is the first level of security established by the organization. This paper proposes what is called a DMZ Firewall to protect the resources from external world. The "DMZ" refers to "De Militarized Zone" which literally means that Military Operations are not conducted with in the Network. This way the "DMZ" acts as a Layer, shielding the Network from the Military Activities, in our case, it is the un-necessary intrusions and threats to the system. Hence the "DMZ" layer is also called the "Perimeter firewall". The way the DMZ Firewall works is that it filters the access of the external systems, based on the regional level access that has been granted to those systems. Hence, as a Cloud Provider, DMZ Layer, acts as the primary step in the Security and protection of network that it can offer to the Customers.

Server Level Security:

The comparison between the Network and Server Level security can be easily understood in broad terms as this: Network applies to the WAN (Wide Area Network) and Server Level Security applies to the LAN (Local Area Network). Hence the protection of physical assets is the next level of Security that the Cloud network / provider should be considering for securing the Customer information. The primary level of assets include the actual servers (Application Servers) and the Database Servers. Application Servers are those Servers, where the Cloud Application actually resides. The Application could be the Web Application that Users would be connecting or the Server version of the Software and installable that the Cloud Provider actually provides its Customers.

This paper proposes the Hyper-V Servers for hosting the Application Server. Hyper-V servers are the Managed Services or Managed Servers. In other words Hyper-V's are virtual or partitioned Servers. The following are the full advantages of using the Hyper-V or the virtual server over using a traditional physical box / stand-alone servers:

1. Cost savings: As Hyper-V's work out much simpler and cheaper solutions when compared with traditional servers, bringing increased savings to the cloud provider
2. Space Advantages: Hyper-V's save a lot of space and hence cost and it is much ease of setup, as they are virtual and easily configurable
3. More Secure and Ease: The Hyper-V's can be secured with much more ease as it combines or hosts multiple servers within itself and the Security aspects are much more advanced than the traditional standalone Severs.

Now, this Hyper-V's are for the Application Level Data. For storing the actual data (that is the Database Layer) this paper proposes Restricted Zone firewall (RZF). Restricted Zone Firewall (RZF) is additional level of Security established by the Networking division of the company, typically the Network Administrator. RZF is applied for critical digital assets, where in the network administrator groups the Critical Servers, in our case, the Database Servers thus securing the Data to a much greater extent. The RZF has access only to the Application Servers, which, again controlled through Secured access. The penetration of external users/hackers is minimized to a lowest probability, if not nullified. Thus the Data in this model resides within two concrete and discrete firewalls – namely – the DMZ and RZF, thus making the Customer Data completely safe and secure, gaining the Trust of the Customers.

Login or Application Level Security:

The first two security levels are to do with the actual and physical environments. The third level – the Login Level Security – is to do with the Cloud Application itself. Any regular Web or the Client Server based application will have a Login and Password access provided to the Users using the system (figure 2). But this linear way of authentication is highly vulnerable to attacks, as this process is a single layer of authentication and hence leads to easy penetration.

Hence this paper introduces the "Timed Random Access Key" generation, during the login. In this approach the Cloud User, gets an additional level of Security apart from the login and password. In the "Random Access Key" generation, the system generates a random key, which could be a combination of alphabets, numbers and special characters. Now, this combination of alpha-numeral along with the special characters makes the "Key" stronger and much complex to break. The "Timed" aspect signifies that the Random Access Key is valid only for a specified amount of time (like, say, 2 minutes) as set by the Administrator.

So when an authorized (registered) user tries to login the system, the user will be prompted to enter the "Timed Random Access Key". This key will be generated from the cloud network and emailed to the registered email address of the user. The User then enters the password and then the "Random Access Key" emailed to him. This combination is verified within the time limit set and then the user is granted access into the Cloud System. This paper also proposes the usage of Security Certificates like

"SSL" (Secure Sockets Layer) and the more advanced "TLS" (Transport Layer Security). Since these security layers have to be during the level of designing the actual cloud system, this SSL & TLS does not fall completely within the scope of this paper.

Data Level Security:

Data Level Security is the most critical aspect of the whole proposed model (figure 3).The first two security levels being the environment, the third on the application level and the last being on the Data Level. The Data level deals with the Customer information, Health information, Financial information etc., the Data Layer Security becomes the most sensitive and the most important aspect of the whole proposed model. This Data Level security is established through the following three functional modules of the proposed model:

a. Audit Trail: In this functional module the complete log information of users accessing the system is captured as a log and stored in the database. The log information includes user ID accessing the system, time stamp of the login, IP address and geography of the network (table 1). This gives a complete picture and track of users accessing the system from which we can infer the peak usage times, frequency of access of a particular user and duration of stay in the system. Determining the frequency of access will be particularly useful, because the Cloud provider [Administrator] can have a base-line the frequency and timing of the user access (for each user) and the duration of stay and if there is a too much deviation from the base-lined version an alert can be provided to the primary and secondary contacts of the user to check to see if the last login is actually a valid or an authorized login, thus ensuring complete control over unintended or unauthorized access into the cloud system.

b. Clustered / Load Balanced Database Servers: By clustering and load balancing the database server, the data is mirrored in another server, thus ensuring back-up during contingency and helps in a great extent during performance and load issues. Even though the concept of elastic cloud storage is beneficial proper balancing of load within the infrastructure is to be implemented.

The proposed system is the implementation set-up in a private cloud network. The process starts up with the access control set up and its pre-requisites. Once the verification process is done, the user is given access to enter the network and can use the applications provided in the cloud. So a proper model must be implemented such that each user access, timing control, storage control, access control, data availability, other user requests, data security, data storage and retrieval must all be properly monitored (figure 4). To have a control over all the events within the private cloud, in the implementation, there is an inclusion of the My-SQL Database server. This is the audit trial scenario that is implemented to have the control over the overall cloud network and the activities inside the network.

Data Aberration Detection Algorithm:

Data must always be stored with the pre-defined rules of the data set. The data security becomes an area of concern when these does scenarios does not match. This modification of data must be in control both to the user and also by the cloud provider. The security and privacy in cloud is being enhanced and newer architecture model proposals is a much important aspect as the overall cloud network is considered a vulnerable model Newer implementations are based on the newer threats to the data that is being stored in cloud and also with regard to the access mechanisms. The data aberration is detected in this cloud network by the usage of My-SQL Database.

Steps for detection algorithm are as follows:

Input: Input is the Data Set D

- Given a data set D containing collection of objects
- Set the condition for the presence and the absence of data/ object For eg: Data unavailability during a server back-up or data unavailable during retrieval process..
- Monitor the user login and the size of the data that is being stored.
- If the records are saved as with time factor and based on the size, the variation resulting in the size of the data stored is calculated and hence the data aberration is monitored and prevented
- The duplicate records that is being stored, or same data set stored with different names can be easily studied if there is an existion condition in the My-SQL database.

given data set are detected in the anomaly detection.

There are various applications that this algorithm can be implemented like the anomaly detection plays a vital role in major areas like Health Care Record Maintenance, Banking(Credit card access and overall bank transactions for the user), Image storage/ Retrieval, Marketing Management, Stock Value assessment, Travel Booking Maintenance.

Performance Evaluation Measures:

Audit Trials- Usage Reports:

The SQL data base being implemented is used as a monitoring agent where in the audit- trial reports are generated whenever there is a need. The following table(1) describes one such user report that the cloud service provider manages. Anomaly.

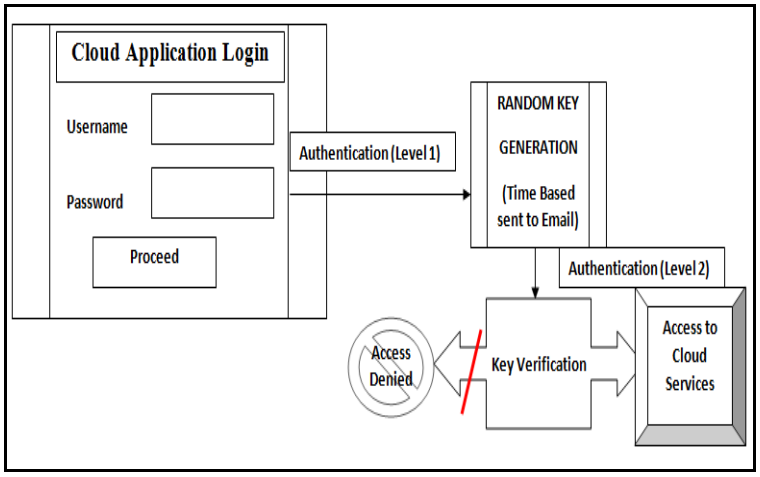

Fig. 2: Login Model.

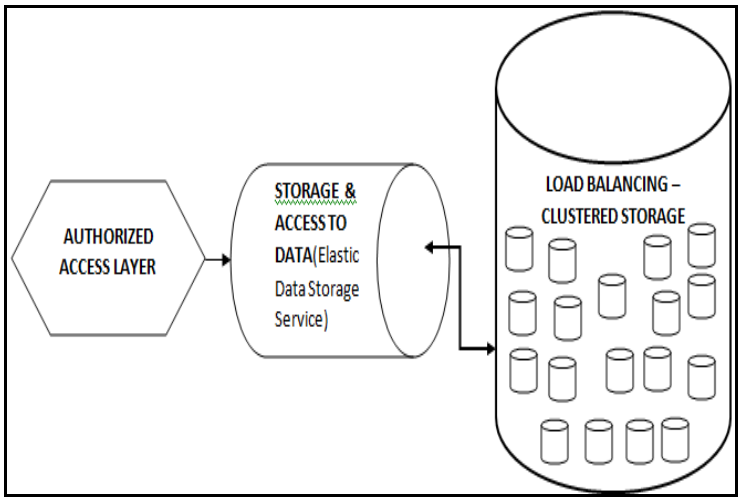

Fig. 3: Data Storage Model.

Implementation Process:

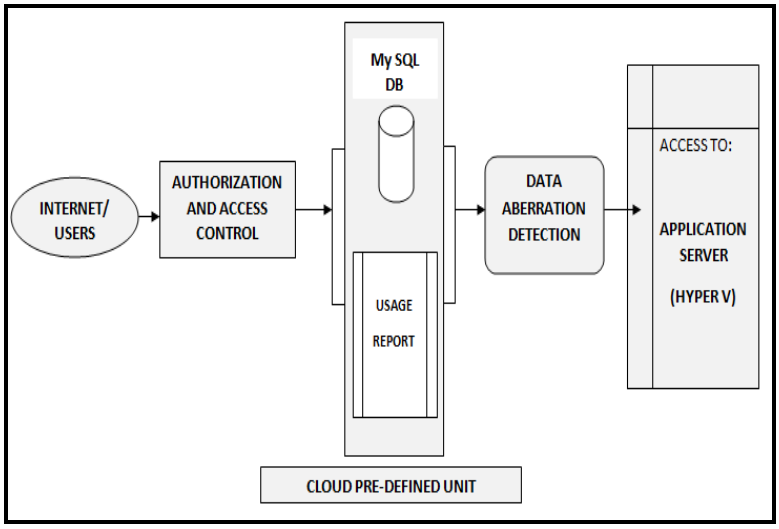

Fig. 4: Implementation Set-UP.

Table 1: Reports from SQL Database

USER	VALIDATION	TIME(LOGIN)
121.19.132.0	YES	01.00
121.19.132.1	YES	12.05
121.19.132.2	YES	16.32
121.19.132.3	YES	09.15
121.19.132.4	YES	14.26

Table 2: Reports of User storage from SQL Database.

RANDOM KEY	LOCATION	DATA SIZE(kb)
abxrrr446u	05.68771 00	1323
1ertg788ig	1.62076 2	558
Y7uh4gt6sa	05.52341 00	889
7yfak9y7l0	001.60019	2357
Ju7tcx85f7	49 4 05.44	998.80

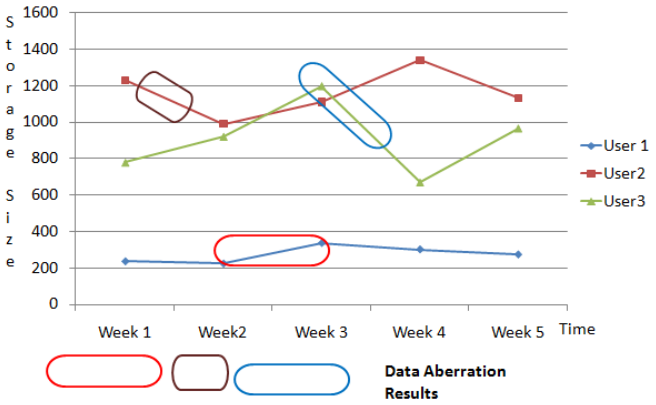

Fig. 5: Aberration Detection.

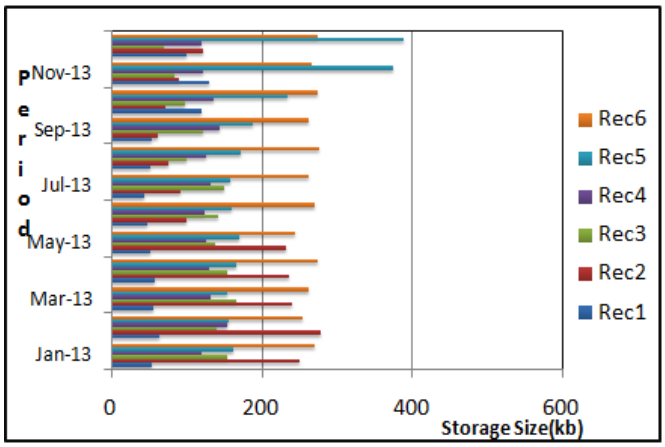

Fig. 6: Analysis of Record Pattern.

Aberration Detection Measures:

The graph shown in the (figure 5). is a representation of data aberration being detected based on the usage as with variations in time to the amount of data that is being stored and retrieved.

The behavioural patterns are pre-defined in the data base and hence monitoring of these variations are being used for data security and data integrity for storage(Fig 6) in the cloud, The data as such can also be stored in a reduced size format and also with some cryptographic encryption methods can be implemented so that the data is stored is secured and retrieval is also secured. Hence the concepts od data security and vulnerability scenarios are also addressed in this model that is beneficial to users of the cloud and to the service providers as well.

Conclusion:

This project proposes Secured Infra-Structure on various layers that form an overall step-by-step authentication and validation in all the cloud model. The future of this work can be implemented in the simulation tool like OPNET where the working of security at various levels and validating the login

each time needed is clearly simulated. The encrypting of data along with the required format of storage can also be included as that scenario is also needed for data integrity. Thus this overall model is based on the current vulnerable model of cloud and is effective as it covers all the levels in the cloud network. The data from the point of its creation till the end of its life span is addressed.

REFERENCES

Benson, Shacham, 2011. "Do you know where cloud files are", PROC 3rd ACM Workshop on Cloud Computing Security-2011.

Butt, S., 2012. "Self-service cloud computing," in Proc. 2012 ACM Computer Communication Security Conf.

Cong Wang, Qian Wang, Kui Ren, Ning Cao and Wenjing Lou, 2012. "Toward Secure and Dependable Storage Services in Cloud Computing", ieee transactions on services computing, 5(2).

Grobauer, B., 2011. "Understanding Cloud Computing Vulnerabilities", Security & Privacy IEEE, vol 9.

Jiadi, Yu., Lu. Peng, 2013. All Toward Secure Multikeyword Top-k Retrieval over Encrypted Cloud data ieee transactions on dependable and secure computing, 10(4).

John Harauz., 2009. Data Security in the World of Cloud Computing JULY/AUGUST, pp: 1540-7993. Published by the IEEE Computer and reliabilty services.

Joseph Idziorek, F. Mark Tannian and Doug Jacobson, "2013. The Insecurity of Cloud Utility Models", Publ ished by the IEEE C omputer Society, pp: 1520-9202.

Khaled Salah, M. Jose Alcaraz Calero, Sherali Zeadally, Sameera Al-Mulla and Mohammed Alzaabi, 2013. "Using Cloud Computing to Implement a Security Overlay Network", Copublished by the IEEE Computer and Reliability Societies, pp: 1540-7993.

Kwang Mong, 2012. Agent-Based Cloud Computing IEEE transactions services computing, 5(4), october-december.

Lan Zhou, Vijay Varadharajan and Michael Hitchens, 2013. "Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage", ieee transactions on information forensics and security, 8(12).

Lori Kaufman, M., Bruce Potter, 2011. "Monitoring Cloud Computing by Layer, Part 1 & 2" ieee computer and reliability societies, pp: 1540-7993.

Luca Ferretti, Michele Colajanni and Mirco Marchetti, 2014. "Distributed, Concurrent, and Independent Access to Encrypted Cloud Databases", ieee transactions on parallel and distributed systems, 25(2).

Song, Fu., 2011. "Performance Metric Selection for Autonomic Anomaly Detection on Cloud Computing Systems", IEEE Global Telecom Conference-2011.

Vijay Varadharajan, Udaya Tupakula, 2014. "Security as a Service Model for Cloud Environment", ieee transactions on network and service management, 11(1).

Virol Negru, 2012. "An Event Driven Multi-Agent Architecture for Enabling Cloud Governance", IEEE/ACM International Conference on Utility and Cloud Computing- 2012.

Wang, C., K. Ren, 2011. "Security and Practical Outsourcing of Linear Programming in Cloud Computing", In IEEE Transactions Cloud Computing April- 2011.

Wayne, A., EMC. Pauley, 2010. "Cloud Provider Transparency -An Empirical Evaluation", ieee computer and reliability societies, pp: 1540-7993.

Zahid Anwar and Asad Waqar Malik, 2014. "Can a DDoS Attack Meltdown My Data Center? A Simulation Study and Defense Strategies", IEEE COMMUNICATIONS LETTERS, 18(7).

Zhang, Y., 2012. "Cross-VM side channels and their use to extract private keys," in 2012 ACM Computer Communication Security Conf.

Zhifeng Xiao and Yang Xiao, 2013. "Security and Privacy in Cloud Computing", ieee communications surveys & tutorials, 15(2).